UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/651,901	08/30/2000	Mariusz H. Jakubowski	MS1-516US	2176

22801 7590 03/05/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
QUINONES, EDEL H	

ART UNIT	PAPER NUMBER
2131	4

DATE MAILED: 03/05/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PRE

Office Action Summary	Application No.	Applicant(s)	
	09/651,901	JAKUBOWSKI ET AL.	
	Examiner	Art Unit	
	Edel H Quinones	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

III. Detailed Action

1. Claims 1-40 are presented for examination.

Information Disclosure Statement

2. The information disclosure statement filed on 6/13/2003 complies with the provisions of MPEP § 609. It has been placed in the application file, and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 10 and 26 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. In the process:

Start with $x = x_0$

Cks := $f(x_0)$ XOR x_0

For i= 1 to K do

$x_i := g(f(x_i\text{-}1))$

Cks += $f(x_i)$ XOR x_i

End for,

it is not clear whether "(x_i-1)" should read "(x_{i-1})" (i.e. with both the "i" and the "-1" as subscripts) or not. For examination purposes, it is assumed that "(x_{i-1})" is the correct one.

Also there is no clear indication as to what the "+=" operator stands for. For examination purposes it is assumed that it stands for: Cks = Cks + $f(x_i)$ XOR x_i

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-4, 6-7, 10-20, 22-23 and 26-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ackerman (U.S. Patent 6,256,777) in view of Richardson (U.S. Patent 5,054,787).

In regards to claims 1, 13, 16-17, 30-31 and 35, Ackerman teaches a system that:

identifies a plurality (i.e. records a list) of key instructions in a function (i.e. locations in machine code where variables need to be saved) (col. 4, lines 41-44);

inserting into the function, for each of the plurality of key instructions, an extra instruction (i.e. placing hidden breakpoints into the machine code) (col. 4, lines 56-57) that modifies a register (i.e. the action might be a manipulation of registers) (col. 4, lines 47-48) based at least in part on the corresponding key instruction (i.e. debugger using debug information file which lists all such breakpoints) (col. 4, lines 61-63).

Ackerman does not teach identifying a set of inputs to the function and determining a checksum for the function based at least in part on mapping contents of the register to the set of inputs. However, using a checksum based on an input and a value of a register is old and well known in the art as shown by Richardson.

Richardson teaches a system that identifies a set of inputs (i.e. check bytes) to a function and determines a checksum for the function based on mapping contents of the register to the set of inputs (see col. 17, lines 60-67).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the system of Ackerman with the teachings of Richardson to include identifying a set of inputs to the function and determining a checksum for the function based at least in part on mapping contents of the register to the set of inputs with the motivation to verify that the data transfer was good (see Richardson, col. 9, lines 57-60).

In regards to claims 2, 4, 14, 18 and 32, Ackerman teaches that identifying a plurality of key instruction comprises identifying, as a key instruction, each instruction in the function that possibly modifies a register or a flag (see col. 4, lines 41-44).

In regards to claims 3 and 19, Ackerman teaches that identifying a plurality of key instructions comprises identifying, as the plurality of key instructions, a plurality of instructions that each modify one or more registers or one or more flags (see col. 4, lines 41-44).

In regards to claims 4 and 20, Ackerman teaches that inserting comprises inserting each extra instruction in a location within the function so that the extra instruction is executed if the corresponding key instruction is executed (i.e. a hidden breakpoint instruction is inserted immediately above the current machine code instruction) (col. 4, lines 65-66).

In regards to claims 6, 22 and 33, Ackerman teaches that the inserting comprises inserting the extra instruction into the function without altering the control flow of the function (see col. 5, lines 12-25).

In regards to claims 7 and 23, Ackerman teaches that inserting comprises inserting, for at least one of the plurality of key instructions, a plurality of extra instructions (i.e. checkpoints) that modify one or more registers (i.e. the action might be a manipulation of registers) (col. 4, lines 47-48). It can be inferred that if more than one register is to be updated by a key instruction, more than one breakpoint needs to be inserted to save the original values of the registers.

In regards to claims 10 and 26, Ackerman does not teach that the checksum comprises both an initial value x_0 and a calculated value Cks calculated according to:

Start with $x = x_0$

Cks := $f(x_0)$ XOR x_0

For i= 1 to K do

$x_i := g(f(x_i\text{-}1))$

Cks += $f(x_i)$ XOR x_i

End for.

From the above it is understood that the output of one iteration is used to compute the input of the next iteration and that the final value of Cks is a cumulative value of all the previous inputs.

Richardson teaches that the output of one iteration is used to compute the input of the next iteration and that the final value of Cks is a cumulative value of all the previous inputs (i.e. the check byte is matched with a checksum in a register which has been accumulating a summation of all the 33 input bytes) (col. 17, lines 61-63).

Therefore it would have been obvious to apply the teachings of Richardson to the system of Ackerson to include that the output of one iteration is used to compute the input of the next iteration and that the final value of Cks is a cumulative value of all the previous inputs with the motivation to verify that the data transfer was good (see Richardson, col. 9, lines 57-60).

In regards to claims 11, 27, 34, 37 and 40, Ackerman teaches that the function is part of a software program (i.e. source code or machine code) (see col. 3, lines 16-17).

In regards to claim 12, the combination of Ackerman and Richardson teaches generating a checksum on bytes of a digital good without reading the bytes (see Richardson col. 17, lines 60-67).

In regards to claims 15 and 28, the claim limitation is a computer-readable memory comprising computer-readable instructions that direct a computer system to perform the method as recited in claim 13 and 16, therefore the same rejections apply.

In regards to claim 29, Ackerman discloses a production system, comprising:

a memory to store an original program (see Figure 1, #16); and

a production server (see Figure 1, #10) equipped with tool that is used to augment the original program for protection purposes (i.e. insert breakpoints) (col. 4, lines 44-45), the production server being configured to identify a plurality of segments (i.e. locations in machine code where variables need to be saved or where the sequential flow does not match that of source code) (col. 4, lines 42-44).

Ackerman does not teach an oblivious checking protection tool used for the application of oblivious checking to each of the plurality of segments.

Richardson teaches the application of oblivious checking (i.e. checksums on bytes) (see col. 17, lines 60-67).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the system of Ackerman with the teachings of Richardson to

include an oblivious checking protection tool used for the application of oblivious checking to each of the plurality of segments with the motivation to verify that the data transfer was good (see Richardson, col. 9, lines 57-60).

In regards to claim 34, the claim limitation is a client-server system; substantially comprising the system of claim 29 therefore the same rejection applies.

In regards to claim 36, Ackerman and Richardson teach generating a checksum value for the program based at least in part on both a set of inputs to the segment and the contents of a register that results from applying the set of inputs to the program.

Ackerman and Richardson do not explicitly teach comparing the generated checksum value to a stored checksum value and determining that the protected program has been tampered with if the generated checksum value does not match the stored checksum value. However, comparing a generated checksum value to a stored checksum value to determine whether a program was tampered with is old and well known in the art. Therefore, it would have been obvious to one of ordinary skill in the art to modify the system of Ackerman and Richardson to include comparing a generated checksum value to a stored checksum value to determine whether a program was tampered with the motivation to verify the integrity of the software program.

In regards to claim 38, the claim limitation is a computer readable media that substantially implement the system of claim 36 therefore, the same rejections applies.

In regards to claim 39, Ackerman and Richardson teach that the plurality of instruction further cause the processor(s) to repeat the generating, comparing, and determining for a plurality of segments of the digital good (see Richardson, col. 9, lines 58-67).

5. Claims 5 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ackerman in view of Richardson as applied to claims 1 and 16 above, in further view of Suzuki et al. (U.S. Patent 5,809,306 and Suzuki hereinafter).

The combination of Ackerman and Richardson teaches the system of claims 1 and 16 as discussed above.

The combination of Ackerman and Richardson does not teach that the inserting comprises inserting each extra instruction in a location within the functions so that the extra instruction is executed after the corresponding key instruction is executed.

Suzuki teaches inserting an extra instruction in a location within the functions so that the extra instruction is executed after a corresponding key instruction is executed (i.e. a compensation instruction is inserted immediately after a machine language instruction for an arithmetic operation that will possibly cause an overflow) (see col. 15, lines 27-30).

Therefore, it would have been obvious to one of ordinary skill in the art to modify the combination of Ackerman and Richardson to include that the inserting comprises inserting each extra instruction in a location within the functions so that the extra instruction is executed after the corresponding key instruction is executed with the motivation to minimize overhead during execution (see Suzuki, col. 9, lines 5-7).

6. Claims 8-9, and 24-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ackerman in view of Richardson as applied to claims 1 and 16 above, in further view of Kolawa et al. (U.S. Patent 6,085,029 and Kolawa hereinafter).

The combination of Ackerman and Richardson teaches the system of claims 1 and 16 as discussed above.

In regards to claims 8 and 24, the combination of Ackerman and Richardson does not teach that the identifying a set of input comprises identifying a set of input patterns to the function that result in different valid computation paths in the function being taken.

Kolawa discloses a system that relates to automatic instrumentation of software programs (see col. 1, lines 30-31). Kolawa teaches that identifying a set of input comprises identifying a set of input patterns that result in different valid computation paths in the function being taken (i.e. instrumentation routines can be inserted to automatically generate program inputs to achieve full testing of all flow paths in the executable program) (see col. 17, lines 51-54).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the combination of Ackerman and Richardson with the teaching of Kolawa to include that identifying a set of input comprises identifying a set of input patterns that result in different valid computation paths in the function being taken with the motivation to achieve full testing of all paths in the executable program (see Kolawa, col. 17, lines 53-54).

In regards to claims 9 and 25, the combination of Ackerman and Richardson does not teach that the identifying a set of input comprises identifying a set of input patterns to the function that result in all valid computation paths in the function being taken.

Kolawa discloses a system that relates to automatic instrumentation of software programs (see col. 1, lines 30-31). Kolawa teaches that identifying a set of input comprises identifying a set of input patterns to the function that result in all valid computation paths in the function being taken (i.e. instrumentation routines can be inserted to automatically generate program inputs to achieve full testing of all flow paths in the executable program) (see col. 17, lines 51-54).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the Applicant's invention to modify the combination of Ackerman and Richardson with the teaching of Kolawa to include that identifying a set of input comprises identifying a set of input patterns to the function that result in all valid computation paths in the function being taken with the motivation to achieve full testing of all paths in the executable program (see Kolawa, col. 17, lines 53-54).

Other Prior Art Made of Record

7. A. Barnes et al. (U.S. Patent No. 4,172,213) discloses a byte stream selective encryption/decryption device;

B. Hall (U.S. Patent No. 5,126,728) discloses and ADP security device for labeled data;

C. Olah (U.S. Patent No. 3,745,316) discloses a computer checking system.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Points of Contact

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edel H. Quiñones whose telephone number is 703-305-8745. The examiner can normally be reached on M-F (8:00AM-5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheik can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-305-3718.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Edel H. Quiñones
Patent Examiner
Technology Center 2100

March 03, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100